RECEIVED
CENTRAL FAX CENTER

JUN 21 2006

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Messerges et al.
For:	System and Method for Secure and Convenient Management of Digital Electronic Content
Serial No.:	09/942,010
Filed:	August 29, 2001
Examiner:	Sherkat, A.
Art Unit:	2131

CERTIFICATE OF TRANSMISSION

I hereby certify that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office, Fax No. (571) 273-8300 on June 21, 2006.

Tawnee Cleary

June 21, 2006
(Date)

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Attention: Board of Patent Appeals and Interferences

TRANSMITTAL OF APPEAL BRIEF, and
PETITION REQUESTING A TWO MONTH EXTENSION

The enclosed brief is being filed in furtherance of the Notice of Appeal, faxed on February 21, 2006. The present filing date of June 21, 2006, is within the original permissible two month term for filing the present brief, extended an additional two months.

In connection with filing the Appeal brief ($500), and the Petition Requesting a Two Month Extension ($450), a fee in the amount of $950 is believed to be due. The undersigned authorizes the Commissioner and respectfully requests that this fee be charged to deposit account 50-2117. The Commissioner is further authorized to charge any additional fees deemed to be necessary in connection with the proper handling and consideration of the Petition requesting a two month extension, and the enclosed Appeal Brief in support of the appeal from

the Examiner's final rejection, including any underpayments, and/or credit any overpayments to deposit account 50-2117.

Respectfully submitted,

BY: Lawrence C Lg -

Lawrence J. Chapa
Reg. No. 39,135
Phone No.: (847) 523-0340
Facsimile No.: (847) 523-2350

Motorola, Inc.
Mobile Devices
Intellectual Property Department
600 North US Highway 45, W4-35
Libertyville, IL 60048

RECEIVED
CENTRAL FAX CENTER
JUN 2 1 2006

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Messerges et al.	)
		)
For:	System and Method for Secure and Convenient Management of Digital Electronic Content	)
		)
Serial No.:	09/942,010	)
		)
Filed:	August 29, 2001	)
		)
Examiner:	Sherkat, A.	)
		)
Art Unit:	2131	)

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Attention: Board of Patent Appeals and Interferences

APPELLANTS' BRIEF

This brief is in furtherance of the NOTICE OF APPEAL, communicated via facsimile on February 21, 2006.

Any fees required under §41.20, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)):

I REAL PARTY IN INTEREST

II RELATED APPEALS AND INTERFERENCES

III STATUS OF CLAIMS

IV STATUS OF AMENDMENTS

I. REAL PARTY IN INTEREST

The real party in interest in this appeal is Motorola, Inc., a Delaware corporation.

II. RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in this appeal, there are no such appeals or interferences.

III. STATUS OF CLAIMS

A. Status of all claims in the proceeding

1. Claims rejected: 1-53
2. Claims allowed: none
3. Claims withdrawn from consideration but not canceled: none
4. Claims objected to: none
5. Claims canceled: none

B. Identification of claims being appealed

The claims on appeal are: 1-53

IV. STATUS OF ANY AMENDMENTS AFTER FINAL

No amendments have been filed after final.

V. SUMMARY OF INVENTION

A first aspect of the present invention, which is being appealed, pertains to a communication device (202), that is operable in a domain-based digital rights management environment (200; Fig. 2; page 8, lines 4-6). The digital rights management environment (200) includes a processing element (802), a receiver (808), which is coupled to and controlled by the processing element (802), and is operable to receive incoming messages to the communication device (202), and a transmitter (806), which is coupled to and controlled by the processing element (802), and is operable to transmit output messages of the communication device (202). The digital rights management environment (200) additionally includes a digital rights management module (804) coupled to the processing element (802) that controls operation of the communication device (202) within the domain-based digital rights management environment (200), wherein the digital rights management module (804) of the communication device (202) in combination with a domain authority (204) of the domain-based digital rights management environment (200) is operable to selectively add the communication device (202) to a domain (216) having one or more communication devices that share a cryptographic key (page 7, line 31 – page 8, line 2), which is associated with the domain (216), and thus permit the communication device (202) to selectively receive and decrypt digital content (112) based upon membership in the domain (216) using the shared cryptographic key (page 7, line 31 – page 8, line 2).

A further aspect of the present invention, which is being appealed, pertains to a method of operation of a communication device (202) of a domain (216) having one or more communication devices that share a cryptographic key (page 7, line 31 – page 8, line 2), which is associated with the domain and is used to decrypt select digital content, in a domain-based digital rights management environment (200; Fig. 2; page 8, lines 4-6). The method includes the communication device (202) communicating (page 14, lines 14-16) to a domain authority (204) a request to register the communication device into a domain (216), in response to a user request. The

method further includes the communication device receiving (page 14, lines 19-20) over a communications channel a cryptographic key(page 7, line 31 – page 8, line 2) of the domain (216) from the domain authority (204) that links the communication device (202) to the domain (216), if the communication device (202) is determined to have access to one or more valid cryptographic elements (page 8, line 28 – page 9, line 2).

A still further aspect of the present invention, which is being appealed, pertains to a method for registering devices in a domain (216) having one or more communication devices that share a cryptographic key (page 7, line 31 – page 8, line 2), which is associated with the domain (216) and is used to decrypt select digital content, in a domain-based digital rights management environment (page 8, lines 4-6; FIG. 2). The method includes a domain authority (204) receiving a request (page 14, lines 14-16) to add a communication device (202) to the domain (216). The domain authority (204) then determines whether the communication device (202) is legitimate by verifying that the communication device (202) has access to one or more valid cryptographic elements (page 8, line 28 – page 9, line 2). If the communication device (202) is determined to be valid, the domain authority (204) transmits (page 14, lines 19-20) over a communications channel to the communication device a cryptographic key (page 7, line 31 – page 8, line 2) of the domain (216) operable to link the communication device (202) to the domain (216).

Yet a still further aspect of the present invention, which is being appealed, pertains to a domain-based digital rights management system (FIG. 4). The domain-based digital rights management system (FIG. 4) includes a communication device (202) linked via a first communications link (FIG. 4) to a domain-based digital rights management environment (200; 210, 404, 406). The communication device (202) includes a processing element (802); a receiver (808), coupled to and controlled by the processing element (802), operable to receive incoming messages to the communication device (202); a transmitter (806), coupled to and controlled by the processing element (802), operable to transmit output messages of the communication device (202); and a digital rights management module (804) coupled to the processing element that controls operation of the communication device (202) within the domain-based digital rights management system (FIG. 4). The domain-based digital rights management system (FIG. 4) further includes a domain authority (204) coupled to the communication device (202) via a second communications link (FIG. 4),

wherein the digital rights management module (804) of the communication device (202) in combination with the domain authority (204) are operable to selectively add the communication device (202) to a domain (216) having one or more communication devices that share a cryptographic key (page 7, line 31 – page 8, line 2), which is associated with the domain (216), and thus permit the communication device (202) to selectively receive and decrypt digital content based upon membership in the domain (216) using the shared cryptographic key (page 7, line 31 – page 8, line 2).

Lastly, the present invention, which is being appealed, pertains to a method of limiting access to digital content in a domain-based digital rights management environment (FIG. 2; page 8, lines 4-6). The method includes a first communication device (202), of a domain (216) having one or more communication devices (202) that share a cryptographic key (page 7, line 31 – page 8, line 2) of the domain (216), requesting digital content. The method further includes verifying authenticity of the domain (216), in response to the request from the first communication device (page 12, lines 8-9), and upon verifying the authenticity of the domain (216), making the requested digital content accessible to the first communication device (202) by binding an encrypted form of the requested digital content to the cryptographic key (page 7, line 31 – page 8, line 2) of the domain (216) to which the first communication device (202) is registered (page 12, lines 11-13).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Whether claims 1-13, 15-32, 34-36 and 38-53 have been improperly rejected under 35 U.S.C. 102(e) as being anticipated by Sweet et al. (US Patent Application Publication No. 2002/0031230).

2. Whether claim 14, 33 and 37 has been improperly rejected under 35 U.S.C. 103(a) as being unpatentable over Sweet et al. (US Patent Application Publication No. 2002/0031230), in view of Tokue et al. (US Patent Application Publication No. 2002/0002413).

VII. ARGUMENTS

A. Rejections under 35 U.S.C. 102

A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). The identical invention must be shown in as complete detail as is contained in the ... claim. Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

1. Whether claims 1-13, 15-32, 34-36 and 38-53 have been improperly rejected under 35 U.S.C. 102(e) as being anticipated by Sweet et al. (US Patent Application Publication No. 2002/0031230).

In attempting to reject the claims, the Examiner has alleged that Sweet et al., '230, makes known each of the features of the claims. However contrary to the Examiner's assertions, Sweet et al., '230, fails to make known each and every feature of the claims. It is not enough to show that some or all of the elements (or similarly named elements) are present in a reference, but the elements need to be used and arranged in a manner, which is contextually consistent with which the elements are used in the claims. Here, the Examiner has focused on vague disconnected statements, and has attempted to impute meaning, which is simply not supported by the actual teaching when considered in context, and/or to apply the teaching to the claim without regard as to the claimed context. Still further, the Examiner has failed to establish that any of the relied upon teachings from the reference are entitled to a date, which would establish the same as a prior teaching. It is noted that the reference relies upon the provisional filing date in order to predate the present application's priority claim, but that not all of the relied upon teachings can be shown to be fully supported by a sufficiently early US filing from which the reference claims priority.

More specifically, the teachings of Sweet et al., '230, continue to be misapplied to the above noted claims in attempting to suggest that the same are anticipated, as presently pending.

While the present application generally provides for a cryptographic key, which is shared by the one or more communication devices of a domain, which enables the digital content to be received and decrypted by the communication devices of the domain, Sweet et al., '230, does not similarly provide for such a cryptographic key, which is shared by the entities, which could be characterized as including one or more communication devices, or which form a domain for purposes of accessing domain authorized content. Alternatively, Sweet et al., '230, includes a working key, which is generally unique for each data object including information of interest (see pg. 1, par. [0011]). Sweet et al., '230, in addition to including a working key, further includes credential keys, which may limit access to portions of a data object (see pg. 1, par. [0014]), dependent upon the set of credentials in a particular user's member profile, that is generally unique for each user (see pg. 3, par. [0035]).

To the extent that Sweet et al., '230, discusses domain level access, the access is generally associated with access to an encrypted header file, which is associated with an encrypted data object, but is not the same as the encrypted data object (see pg. 9, par. [0132]). The cited reference then provides that read and write access to the encrypted data object are then preferably accomplished through the use of pseudo-random value encryption keys, which are based upon credential keys (see pg. 9, par. [0133]), which as noted above are further based upon the set of credentials contained in each member profile, which is unique to each user.

At best, the encrypted data object, identified in the cited reference, and not the associated header file, is more closely akin to content. Consequently a domain level of access to a header file is not the same as providing a shared domain-level cryptographic key, which enables the receipt and decryption of digital content, based upon membership in the domain, as provided by the claims of the present application. "Content" is defined by the American Heritage Dictionary of the English Language, Fourth Edition, published by the Houghton Mifflin Company (2000), as "the substantive or meaningful part". Alternatively, "header" is defined by the Free On-line Dictionary of Computing, Denis Howe, (1993-2004), as "the portion of a packet, preceding the actual data" and "the part of an electronic mail message or news article that precedes the body of a message". Hence, one skilled in the art would not recognize header information as being equivalent to content.

Even at a more basic level, the use of the term domain in the cited reference relates to a group of members identified through individual member accounts, which is silent as to "having one or more communication devices", as provided by the claims of the present application. While the present application describes members as having individual member accounts and corresponding member tokens, no such designation is described relative to one or more various communication devices. In fact, the present application envisions that a particular user may have more than one communication device (see pg. 8, lines 2-3), which in turn can be enrolled in the same domain. The cited reference is silent as to any relationship of one or more "communication devices" relative to a domain. As noted above, it is the association with a member account which establishes access through one or more assigned credentials, which is different than being based upon association with a domain including one or more communication devices.

The above noted-inconsistencies between the cited reference and the present application make generally inapplicable the teaching of the reference in attempting to make known or obvious any of the claims of the present application. Consequently, Sweet et al., '230, fails to support an alleged anticipation of each of the independent claims, as well as each of the corresponding dependent claims, which depend therefrom.

In responding to applicants' previous arguments, the Examiner has mischaracterized the Applicants position and correspondingly failed to address the specific deficiencies noted by the applicants, namely the failure to provide for a shared cryptographic key used by a domain having one or more communication devices. Instead the Examiner focuses on "encrypted content" in isolation without reference to a claimed context, which is relevant to the claims of the present application, where the encrypted content is encrypted and decrypted using a domain based key. The Examiner further focuses on the possibility that a member may have multiple devices, but then fails to show how the multiple devices form a domain, which has a corresponding shared cryptographic key, based upon the domain of devices. As noted above and supported by the portion of the reference specifically cited by the Examiner, paragraph [0172], the common content is accessible through appropriate credentials associated with a member account, and not a particular domain having one or more devices. It is the credentials associated with the user that allows the user to access the content using client application software for his player devices. The

requirement of credential keys in the cited reference seems to preclude a shared cryptographic key, which is associated with the domain of one or more communication devices.

Furthermore the focus on the portion of the reference, paragraph [0146], which identifies examples of a member's client system, as including personal computer, cellular telephone or wireless personal digital assistant, similarly fails to support a teaching of a domain having one or more communication devices, in so far, as a more complete reading of the paragraph further provides that the member's credentials would never need to be transmitted to member systems, which further suggests that the concept of domain as taught by the reference is organized, based upon being a particular member (i.e. a particular user) and not the device. Such that a domain in the context of the reference fails to correspond to a claimed context, which associates the claimed domain and the one or more devices that share the cryptographic key.

Consequently, contrary to the assertions of the Examiner, Sweet et al., '230, fails to make known each and every feature of the claims in a manner which is contextually consistent, regardless as to whether the Examiner can properly establish that each of the teachings being relied upon can be shown to be entitled to a sufficiently early US filing date to constitute a prior teaching.

B. Rejections under 35 U.S.C. 103

The Examiner has rejected claims 14, 33 and 37 under 35 U.S.C 103(a) as being unpatentable over Sweet et al., '230, in view of Tokue et al., '413. However, in each instance, the rejection has been misapplied. The specific reasoning outlining the misapplication of the rejections are noted below.

The Federal Circuit has repeatedly emphasized that, with respect to obviousness, the standard for patentability is the statutory standard. The inquiry is whether the claimed subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art. In this regard, see for example, Monarch Knitting Machinery Corp. v. Saulzer Maurat GMBH, 139 F.3d 877, 881, 45 USPQ2d 1977, 1981 (Fed. Cir. 1998).

For purposes of formulating an obviousness type rejection, the Patent and Trademark Office (PTO) has the initial burden of presenting a prima facie case. In re Mayne, 104 F.3d 1339, 1341, 41 USPQ2d 1451 (Fed. Cir. 1997). In order to establish a prima facie case of obviousness, it must be shown that the prior art reference, or references when combined, teach or suggest all of the claim limitations. Pro-Mold and Tool Co. v. Great Lakes Plastics Inc., 75 F.3d 1568, 37 USPQ2d 1626, 1629 (Fed. Cir. 1996), In re Royka, 490 F.2d 981, 180 USPQ 580, 583 (CCPA 1974). Furthermore, the showing of a suggestion, teaching, or motivation to combine prior teachings "must be clear and particular." In re Dembiczak, 175 F.3d 994, 50 USPQ2d 1614 (Fed. Cir. 1999). These requirements are consistent with the Patent and Trademark Office's own examination guidelines governing the formation of obvious type rejections, see MPEP §2142.

2. Whether claim 14, 33 and 37 has been improperly rejected under 35 U.S.C. 103(a) as being unpatentable over Sweet et al. (US Patent Application Publication No. 2002/0031230), in view of Tokue et al. (US Patent Application Publication No. 2002/0002413).

Despite the Examiner's assertions to the contrary, for purposes of serving as a basis of a prior teaching, a foreign priority date is simply not relevant. Consequently, any teaching associated with Tokue et al., '413, cannot be established as constituting a prior teaching, and therefore any reliance on the part of the Examiner of the reference in support of a rejection is entirely inappropriate. Please note, the US filing date of the reference, Tokue et al., '413, is June 27, 2001, which is after the priority date (April 18, 2001) of the present application. Therefore, the examiner has failed to properly allege a corresponding rejection, which is fully supported by a properly relied upon reference, which could be said to constitute a prior teaching that is relevant to the prosecution of the present application.

Consequently, any feature of the claims that the reference is relied upon for purposes of supporting an assertion that the same is known or obvious, can not be said to be properly supported, so as to be relevant to the present application. Consequently the corresponding rejection should be reversed.

In view of the above analysis, the applicants would assert, that the Examiner has failed to establish that any of the cited references either separately or in combination make known or obvious any of the presently pending claims. The applicants would respectfully request that the Examiner's decision to finally reject the presently pending claims be overturned, and that the claims be permitted to proceed to allowance.

Respectfully submitted,

BY: _____

Lawrence J. Chapa
Reg. No. 39,135
Phone No.: (847) 523-0340

Motorola, Inc.
Mobile Devices
Intellectual Property Department
600 North US Highway 45, AS437
Libertyville, IL 60048

VIII. CLAIMS APPENDIX

The following is the text of the claims involved in this appeal:

1. A communication device operable in a domain-based digital rights management environment, comprising:

a processing element;

a receiver, coupled to and controlled by the processing element, operable to receive incoming messages to the communication device;

a transmitter, coupled to and controlled by the processing element, operable to transmit output messages of the communication device; and

a digital rights management module coupled to the processing element that controls operation of the communication device within the domain-based digital rights management environment;

wherein the digital rights management module of the communication device in combination with a domain authority of the domain-based digital rights management environment is operable to selectively add the communication device to a domain having one or more communication devices that share a cryptographic key, which is associated with the domain, and thus permit the communication device to selectively receive and decrypt digital content based upon membership in the domain using the shared cryptographic key.

2. The communication device of claim 1, wherein the transmitter is a limited range transmitter having a limited communication range and operable to transit the digital content to a trusted communication device within the limited communication range.

3. The communication device of claim 1, wherein in response to receiving a user request, the digital rights management module causes the transmitter of the communication device to transmit to a domain authority a request to register the communication device into the domain; and

wherein if the communication device is determined to have access to one or more valid cryptographic elements, the digital rights management module causes the receiver of the communication device to receive over a communications channel the cryptographic key of the domain from the domain authority to link the communication device to the domain.

4. The communication device of claim 3, wherein the digital rights management module in combination with the domain authority removes the communication device from the domain, comprising:

in response to the request of the user of the domain to remove the communication device, the digital rights management module of the communication device causes the transmitter to transmit a request that the communication device be removed from the domain;

in response to the request that the communication device be removed from the domain, the communication device receives from the domain authority via the secure communications channel a command to remove the cryptographic key of the domain from the communication device; and

upon receiving the command from the domain authority, the digital rights management module of the communication device removes the cryptographic key of the domain.

5. The communication device of claim 1, wherein in response to the digital rights management module of the communication device causing the transmitter to transmit a request for digital content, at least one of the digital rights management module of the communication device and the domain authority verifies authenticity of the domain; and

wherein upon verification of the authenticity of the domain, the receiver of the communication device receives an encrypted form of the requested digital content that is bound to the cryptographic key of the domain in which the communication device is registered.

6. The communication device of claim 1, wherein the digital rights management module of the communication device enforces usage rules associated with the requested digital content and received by the receiver in a content package containing the requested digital content.

7. The communication device of claim 6, wherein the content package comprises a binary representation rights table that contains the usage rules.

8. The communication device of claim 7, wherein the binary representation rights table comprises a plurality of sections having predefined tokens.

9. The communication device of claim 1, wherein the digital rights management module, in response to the transmitter of the communication device receiving a request from a second communication device of the domain requesting the digital content, causes the transmitter to transmit the requested digital content from a storage element to the second communication device.

10. The communication device of claim 1, wherein in response to a request of the user of the communication device, the digital rights management module causes the transmitter to transmit a request for digital content that is not available in the domain; and

wherein after authenticity of the domain has been verified, the receiver receives an encrypted form of the requested digital content that is bound to the cryptographic key of the domain to which the communication device is registered.

11. The communication device of claim 10, wherein the encrypted form of the requested digital content is contained in a content package.

12. The communication device of claim 11, wherein the content package further comprises a binary representation rights table that contains the usage rules of the requested digital content.

13. The communication device of claim 12, wherein the binary representation rights table comprises a plurality of sections having predefined tokens.

14. The communication device of claim 10, wherein the digital rights management module of the communication device stores the encrypted digital content in an open-access storage element.

15. The communication device of claim 10, wherein the digital rights management module of the communication device enforces usage rules associated with the requested digital content and received by the receiver in a content package containing the requested digital content.

16. The communication device of claim 15, wherein the content package comprises a binary representation rights table that contains the usage rules.

17. The communication device of claim 16, wherein the binary representation rights table comprises a plurality of sections having predefined tokens.

18. The communication device of claim 1, wherein in response to the receiver receiving a request from a second communication device of the one or more communication devices of the domain for the digital content and the digital rights management module verifying the authenticity of the second communication device, the digital rights management module causing the transmitter to transmit the requested digital content from a storage element of the communication device to the second communication device.

19. The communication device of claim 1, wherein the digital rights management module causes digital legacy content received from a source external to the domain to be stored in a storage element of the communication device; and

wherein in response to a request from a second communication device of the domain, the digital rights management module causes the transmitter to transmit the digital legacy content from

the storage element to the second communication device.

20. A method of operation of a communication device of a domain having one or more communication devices that share a cryptographic key, which is associated with the domain and is used to decrypt select digital content, in a domain-based digital rights management environment, comprising:

in response to a user request, the communication device communicating to a domain authority a request to register the communication device into a domain; and

if the communication device is determined to have access to one or more valid cryptographic elements, the communication device receiving over a communications channel a cryptographic key of the domain from the domain authority that links the communication device to the domain.

21. The method of claim 20, further comprising:

the communication device, of a domain having one or more communication devices that share a cryptographic key of the domain, requesting digital content;

in response to the communication device requesting digital content, at least one of the communication device and the domain authority verifying authenticity of the domain; and

upon verification of the authenticity of the domain, the communication device receiving an encrypted form of the requested digital content that is bound to the cryptographic key of the domain to which the communication device is registered.

22. The method of claim 21, further comprising the communication device enforcing

usage rules associated with the requested digital content and received in a content package containing the requested digital content.

23. (previously presented) The method of claim 22, wherein the content package comprises a binary representation rights table that contains the usage rules.

24. The method of claim 23, wherein the binary representation rights table comprises a plurality of sections having predefined tokens.

25. The method of claim 21, further comprising:

a second communication device of the one or more communication devices of the domain requesting the digital content; and

transferring the requested digital content from a storage element to the second communication device.

26. The method of claim 20, wherein removing the communication device from the domain comprises:

in response to the request of the user of the domain to remove the communication device, the communication device transmitting a request that the communication device be removed from the domain; and

in response to the request that the communication device be removed from the domain, the communication device receiving from the domain authority via the secure communications channel a

command to remove the cryptographic key of the domain from the communication device.

27. The method of claim 26, further comprising:

upon receiving the command from the domain authority, the communication device removing the cryptographic key of the domain.

28. The method of claim 20, wherein prior to the communication device communicating to a domain authority the request to register the communication device into the domain, further comprising the communication device:

communicating to the domain authority a request to establish the domain, said request having a domain name and a domain password;

communicating to the domain authority via a communications channel a unique identifier of the communication device;

downloading the cryptographic key created by the domain authority;

29. The method of claim 20, further comprising:

in response to a request of the user of the communication device, the communication device requesting digital content that is not available in the domain; and

after authenticity of the domain has been verified, the communication device receiving an encrypted form of the requested digital content that is bound to the cryptographic key of the domain to which the communication device is registered.

30. The method of claim 29, wherein the encrypted form of the requested digital content is contained in a content package having usage rules enforced by the communication device.

31. The method of claim 29, wherein the content package comprises a binary representation rights table that contains the usage rules.

32. The method of claim 31, wherein the binary representation rights table comprises a plurality of sections having predefined tokens.

33. The method of claim 29, further comprising the communication device storing the encrypted digital content in an open-access storage element.

34. The method of claim 29, further comprising:

the communication device receiving a request from a second communication device of the one or more communication devices of the domain requesting the digital content;

the communication device verifying the authenticity of the second communication device; and

if the authenticity of the second communication device is verified, the communication device transferring the requested digital content from a storage element of the communication device to the second communication device.

35. The method of claim 20, further comprising:

the communication device receiving digital legacy content from a source external to the domain and storing it in a storage element of the communication device; and

in response to a request from a second communication device of the domain, the communication device transmitting the digital legacy content from the storage element to the second communication device.

36. A method for registering devices in a domain having one or more communication devices that share a cryptographic key, which is associated with the domain and is used to decrypt select digital content, in a domain-based digital rights management environment, comprising:

a domain authority receiving a request to add a communication device to the domain;

the domain authority determining whether the communication device is legitimate by verifying that the communication device has access to one or more valid cryptographic elements;

if the communication device is determined to be valid, the domain authority transmitting over a communications channel to the communication device a cryptographic key of the domain operable to link the communication device to the domain.

37. The method of claim 36, wherein prior to the domain authority transmitting the cryptographic key to the communication device further comprising:

The domain authority determining that the one or more communication devices of the domain do not exceed a predetermined upper limit.

38. The method of claim 36, further comprising prior to receiving a request to add the

communication device to the domain, the domain authority receiving a request to create the domain having a domain name and a domain password;

the domain authority initiating the communications channel with the communication device;

the domain authority determining a unique identification of the communication device;

the domain authority establishing the domain using the unique identification of the communication device, the domain name, and the domain password;

the domain authority creating the cryptographic key of the domain; and

the domain authority providing the cryptographic key for download by the communication device.

39. The method of claim 36, further comprising:

in response to a communication device of the domain requesting digital content, the domain authority verifying authenticity of the domain.

40. The method of claim 36, wherein removing the communication device from the domain comprises the domain authority:

receiving the request to remove the communication device from the domain;

authenticating the communication device; and

upon authenticating the communication device the domain authority transmitting via a secure communications channel to the communication device a command to remove the cryptographic key of the domain from the communication device.

41. The method of claim 36, further comprising the domain authority:

maintaining a log of requests by the communication device to register to or be deleted from one or more domains;

monitoring the log to identify potentially fraudulent activity by the communication device; and

generating a warning message in response to identifying potentially fraudulent activity by the communication device.

42. The method of claim 41, further comprising revoking a public key of the communication device if the communication device is determined to be engaged in fraudulent activity.

43. A domain-based digital rights management system, comprising:

a communication device linked via a first communications link to a domain-based digital rights management environment, comprising:

a processing element;

a receiver, coupled to and controlled by the processing element, operable to receive incoming messages to the communication device;

a transmitter, coupled to and controlled by the processing element, operable to transmit output messages of the communication device; and

a digital rights management module coupled to the processing element that controls operation of the communication device within the domain-based digital rights management

system;

a domain authority coupled to the communication device via a second communications link;

wherein the digital rights management module of the communication device in combination with the domain authority are operable to selectively add the communication device to a domain having one or more communication devices that share a cryptographic key, which is associated with the domain, and thus permit the communication device to selectively receive and decrypt digital content based upon membership in the domain using the shared cryptographic key.

44. A method of limiting access to digital content in a domain-based digital rights management environment, comprising:

a first communication device, of a domain having one or more communication devices that share a cryptographic key of the domain, requesting digital content;

in response to the request from the first communication device, verifying authenticity of the domain; and

upon verifying authenticity of the domain, making the requested digital content accessible to the first communication device by binding an encrypted form of the requested digital content to the cryptographic key of the domain to which the first communication device is registered.

45. The method of claim 44, wherein the encrypted form of the requested digital content is contained in a content package having usage rules enforced by the first communication device.

46. The method of claim 45, wherein the content package comprises a binary representation rights table that contains the usage rules.

47. The method of claim 46, wherein the binary representation rights table comprises a plurality of sections having predefined tokens.

48. The method of claim 44, wherein prior to the first communication device requesting digital content establishing the domain, said establishing further comprising:

in response to a user request, the first communication device communicating to a domain authority a request to register the first communication device into the domain;

the domain authority determining whether the first communication device is legitimate by verifying that the first communication device has access to one or more valid cryptographic elements; and

the first communication device receiving over a communications link a cryptographic key of the domain from the domain authority that links the first communication device to the domain.

49. The method of claim 44, further comprising:

a second communication device of the one or more communication devices of the domain requesting the digital content; and

transferring the requested digital content from a storage element to the second communication device.

50. The method of claim 44, further comprising:

a second communication device of the one or more communication devices of the domain receiving digital legacy content from a source external to the domain and storing it in a storage element of the second communication device; and

In response to a request from a third communication device of the domain, the second communication device transmitting the digital legacy content from the storage element to the third communication device.

51. The method of claim 44, further comprising removing a second communication device from the domain in response to a request from a user of the domain.

52. The method of claim 51, wherein removing the second communication device from the domain comprises:

in response to the request of the user of the domain to remove the second communication device, the second communication device transmitting a request to the domain authority to remove the second communication device from the domain;

in response to the request that the second communication device be removed from the domain, the domain authority transmitting a command via the secure communications channel to remove the cryptographic key of the domain from the second communication device; and

upon receiving the command from the domain authority, the second communication device removing the cryptographic key of the domain resident on the second communication device.

53. The method of claim 52, wherein the request that the second communication device be removed from the domain is made by the user at a website of the domain authority.

IX. EVIDENCE APPENDIX

None

X. RELATED PROCEEDINGS APPENDIX

None